REMARKS

This paper is responsive to the Office Action dated December 18, 2003. All rejections of the Examiner are respectfully traversed. Reconsideration and further examination is respectfully requested.

At paragraph 2 of the Office Action, the Examiner rejected claims 1-8, 15-22, and 26-49 for anticipation under 35 U.S.C. 102 by United States patent number 5,748,736 of Mittra ("Mittra"). Applicants respectfully traverse this rejection.

Mittra discloses a system for secure group communication via multicast or broadcast transmission. Mittra teaches a secure multicast group consisting of senders, receivers, a group security controller (GSC), and at least one trusted intermediary (TI) server. The GSC and each TI server of the Mittra system are responsible for maintaining the security of the group by authenticating and authorizing all other members of the multicast as well as managing group key(s) that are used to encrypt messages multicast to the group.

Nowhere in Mittra is there disclosed or suggested any system or method for implementing multicast security in a given multicast domain with one or more network devices, that includes processing ***multicast traffic that is encrypted with a global key, the global key being available to the given multicast domain and one or more other multicast domains***, as in the present independent claims 1, 15, 26, 34 and 42. In contrast, beginning at line 61 of column 9, Mittra describes a system that can use one of three types of keys. The first possibility taught by Mittra is a group key that is used to encrypt messages to the group. Accordingly, this is a key known by a single multicast group. A second option proposed by Mittra is the use of a key that is unique to the sender and the GSC. This is a key agreed upon and known by only a single sender

and the GSC. Finally, Mittra discusses the potential for using a key randomly selected by either the sender or by the GSC. None of these options disclosed in Mittra provide any hint or suggestion of even the desirability of having a global key that is available to multiple multicast domains, as in the present independent claims 1, 15, 26, 34 and 42. Moreover, any key other than the group key in Mittra is explicitly described as being unique to a single sender and the GSC.

For the reasons stated above, Applicants respectfully urge that Mittra does not disclose or suggest all the features of the present invention as set forth in independent claims 1, 15, 26, 34 and 42. Accordingly, Applicants respectfully submit that Mittra does not anticipate independent claims 1, 15, 26, 34 and 42 under 35 U.S.C. 102. As to claims 2-8, 16-22, 26-33, 35-41, and 43-49, they each depend from claims 1, 15, 26, 34 and 42, and are believed to be patentable over Mittra for at least the same reasons.

At paragraph 3, the Examiner rejected claims 9-14 and 23-25 as being anticipated under 35 U.S.C. 102 by United States patent number 6,331,983 of Haggerty et al. ("Haggerty et al."). Applicants respectfully traverse this rejection.

Haggerty et al. disclose a system for establishing connections in a switch-based communications network for multicast traffic. As described in Haggerty et al., a source receives a multicast packet on an access port from a source host, determines a group address in the multicast packet, and composes and sends a "sender present" message to other switches on its network ports. The receiving switches of the Haggerty et al. system then determine whether a local host wishes to join the group and if so, send a map message back toward the source switch on a predetermined path between the receiving switch and the source switch.

With regard to independent claims 9 and 23, nowhere in Haggerty et al. is there disclosed or suggested any system or method for implementing multicast security in a given multicast domain with one or more network devices, that includes processing ***multicast traffic that is encrypted with a global key, the global key being available to the given multicast domain and one or more other multicast domains***, as in claims 9 and 23. In contrast, Haggerty et al. discusses the use of a "flow identifier connection key" to distinguish specific types of packets based on its values. See the discussion in Haggerty et al. beginning at line 34 of column 19 regarding the "IGMP Active Senders Problem". This flow identifier connection "key" is again referred to in Haggerty et al. in column 23 in the paragraph beginning at line 26 with regard to detecting multiple sender conditions during connection set up. Thus the "key" used in Haggerty et al. is not related to the above encryption of multicast traffic with the global key feature of the present independent claims 9 and 23.

For these reasons, Applicants respectfully urge that Haggerty et al. do not disclose or suggest all the features of the present independent claims 9 and 23. Accordingly, Haggerty et al. does not anticipate claims 9 and 23 under 35 U.S.C. 102. As to claims 10-14 and 24-25, they each depend from claims 9 and 23, and are believed to be patentable over Haggerty et al. for at least the same reasons. Reconsideration of all pending claims is respectfully requested.

Applicants have made a diligent effort to place the claims in condition for allowance. However, should there remain unresolved issues that require adverse action, it is respectfully requested that the Examiner telephone David A. Dagg, Applicants' Attorney at 978-264-6664 so that such issues may be resolved as expeditiously as possible.

For these reasons, and in view of the above amendments, this application is now considered to be in condition for allowance and such action is earnestly solicited.

Respectfully Submitted,

March 18 2004
Date

David A. Dagg, Reg. No. 37,809
Attorney/Agent for Applicant(s)
Steubing McGuinness & Manaras LLP
125 Nagog Park Drive
Acton, MA 01720
(978) 264-6664

Docket No. 120-111